California
TECHNOLOGY AGENCY
Office of Technology Services

Information Security Officer Meeting
DNS Security Project

Security Management Section

March 8, 2012

California Technology Agency
Office of Technology Services

Agenda

- Background
- Objective
- Milestones
- Solution
- Accomplishments
- Question and Answer

Background

- The Domain Name System (DNS) provides information fundamental to Internet based services for California state and local governments.
- DNS data integrity and source authentication is critical to maintaining Internet based services.
- CA government is vulnerable to DNS attacks.

Background

- Federal mandate to implement DNSSEC – January 2009 (.gov).
- OIS received grant approval for California government to implement DNSSEC – December 2009.
- OTech managed service.

Objective

- To provide the ability to validate the authenticity and integrity of DNS messages.

Milestones

- Document current DNS security infrastructure
- Conduct vulnerability and gap assessment
- Identify solutions that are compatible with federal mandate
- Pilot
- Implementation

Solution

- Infoblox
  - Largest installed base
  - Favorable customer feedback
  - Overall strong rating
  - Selected by Homeland Security
  - Two master redundant appliances
  - Approx. 600 OTech managed domains
  - SHA256: key 2,048 bits renewed yearly; zones 1024 bits renewed monthly

California Technology Agency
Office of Technology Services

Accomplishments

- Federal .gov Authentication
- DNSSEC is the Authoritative DNS for ca.gov
- Managed ca.gov Authenticated

California Technology Agency
Office of Technology Services

Questions and Answers